UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/674,468 | 03/23/2001 | Andrew John Cardno | 6825 | 1245 |

25763 7590 02/11/2004

DORSEY & WHITNEY LLP
INTELLECTUAL PROPERTY DEPARTMENT
50 SOUTH SIXTH STREET
MINNEAPOLIS, MN 55402-1498

| EXAMINER | |
|---|---|
| HOLMES, MICHAEL B | |
| **ART UNIT** | **PAPER NUMBER** |
| 2121 | |

DATE MAILED: 02/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/674,468 | CARDNO, ANDREW JOHN | |
| | Examiner | Art Unit | |
| | Michael B. Holmes | 2121 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *(3)* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *23 March 2001* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-89* is/are pending in the application.

4a) Of the above claim(s) *2-45* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 46-89* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 March 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. *09/674,468* .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *5,8* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

UNITED STATES PATENT AND TRADEMARK OFFICE

P.O. Box 1450, Alexandria, Virginia 22313-1450 - WWW.USPTO.GOV

# Examiner's Detailed Office Action

1. This action is responsive to application **09/674,468,** filed **March 23, 2001**.

2. **Claims 2-45** have been canceled.

3. **Claims 46-89** have been added and examined.

## Information Disclosure Statement

4. Examiner acknowledges applicants' submission of prior art and information disclosure. Nevertheless, applicant is respectfully remind of the ongoing Duty to disclose 37 C.F.R. 1.56 all pertinent information and material pertaining to the patentability of applicant's claimed invention, by continuing to submitting in a timely manner PTO-1449, Information Disclosure Statement (IDS) with the filing of applicant's of application or thereafter.

## Drawings

5. The formal drawings have been reviewed by the United States Patent & Trademark Office of Draftperson's Patent Drawings Review. Form PTO-948 has been provided. Note, in figure 1, items 22, 20, 30, 26 & 28, are not labeled. Appropriate correction is required.

## Specification

6. The specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is required in correcting any errors of which applicant may become aware in the specification. Appropriate correction is required.

## Claim Interpretation

7. Office personnel are to give claims their **"broadest reasonable interpretation"** in light of the supporting disclosure. *In re Morris*, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997). Limitations appearing in the specification but not recited in the claim are not read into the claim. *In re Prater*, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-551(CCPA 1969). See *also *In re Zletz*, 893 F.2d 319, 321-22, 13 USPQ2d 1320, 1322(Fed. Cir. 1989) ("During patent examination the pending claims must be interpreted as broadly as their terms reasonably allow. . . . The reason is simply that during patent prosecution when claims can be amended, ambiguities should be recognized, scope and breadth of language explored, and clarification imposed. . . . An essential purpose of patent examination is to fashion claims that are precise, clear, correct, and unambiguous. Only in this way can uncertainties of claim scope be removed, as much as possible, during the administrative process."). *see* MPEP § 2106

# Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> **(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent,** or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

9. The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

10. **Claims 1, 46-47, 52-54, 59-61, 66, 67-69, 74, 75-77, 82-84 & 89** are rejected under 35 U.S.C. 102(e) as being anticipated by

**Gopinathan et al. (USPN 5,819,226), Filed: Sep. 08, 1992; Date of Patent: Oct. 06, 1998.**

**Regarding Claim 1:**

*Gopinathan et al.* teaches,

An interaction prediction system comprising:

a memory in which is maintained a neural network trained on data retrieved from an interaction database of interaction data representing interactions between customers and merchants; **[FIG. 1 & FIG. 4; (col. 3, line 47-65 "*In accordance with the software program instructions, CPU 101***

***stores the data obtained from data network 105 in data storage 103, and uses RAM 102 in a conventional manner as a workspace. CPU 101, data storage 103, and program storage 107 operate together to provide a*** *neural network* ***model 108 for*** *predicting* ***fraud.*** *After neural network 108 processes the information, as described below, to obtain an indication of the likelihood of fraud, a signal indicative of that likelihood is sent from CPU 101 to output device 104.* ***In the preferred embodiment, CPU 101 is a Model 3090 IBM mainframe computer, RAM 102 and data storage 103 are conventional RAM, ROM and disk storage devices for the Model 3090 CPU, and output device 104 is a conventional means for either printing results based on the signals generated by neural network 108, or displaying the results on a video screen using a window-based interface system, or sending the results to a database for later access, or sending a signal dependent on the results to an authorization system (not shown) for further processing.***") **& (col. 5, line 54 to col. 6, line 6 "***Neural networks learn from examples by modifying their weights. The "training" process, the general techniques of which are well known in the art, involves the following steps: 1) Repeatedly presenting examples of a particular input/output task to the neural network model; 2) Comparing the model output and desired output to measure error; and 3) Modifying model weights to reduce the error. This set of steps is repeated until further iteration fails to decrease the error. Then, the network is said to be "trained."* ***Once training is completed, the network can predict outcomes for new data inputs.*** *Fraud-Related Variables:* ***In the present invention, data used to train the model are drawn from various database files containing historical data on individual transactions, merchants, and customers. These data are preferably pre-processed before being fed into the neural network, resulting in the creation of a set of fraud-related variables that have been empirically***

***determined to form more effective predictors of fraud than the original historical data.")]*** retrieved means arranged to activate the neural network and to retrieve prediction data representing future interactions between customers and merchants; **[(col. 3, line 47-65 "*In accordance with the software program instructions, CPU 101 stores the data obtained from data network 105 in data storage 103, and uses RAM 102 in a conventional manner as a workspace. CPU 101, data storage 103, and program storage 107 operate together to provide a neural network model 108 for predicting fraud. After neural network 108 processes the information, as described below, to obtain an indication of the likelihood of fraud, a signal indicative of that likelihood is sent from CPU 101 to output device 104. In the preferred embodiment, CPU 101 is a Model 3090 IBM mainframe computer, RAM 102 and data storage 103 are conventional RAM, ROM and disk storage devices for the Model 3090 CPU, and output device 104 is a conventional means for either printing results based on the signals generated by neural network 108, or displaying the results on a video screen using a window-based interface system, or sending the results to a database for later access, or sending a signal dependent on the results to an authorization system (not shown) for further processing.*")]** and display means arranged to display a representation of the prediction data. **[(col. 3, line 56-65 "*In the preferred embodiment, CPU 101 is a Model 3090 IBM mainframe computer, RAM 102 and data storage 103 are conventional RAM, ROM and disk storage devices for the Model 3090 CPU, and output device 104 is a conventional means for either printing results based on the signals generated by neural network 108, or **displaying the results on a video screen using a window-based interface system**, or sending the results to a database for later access, or sending a signal dependent on the results to an authorization system (not shown) for further pro-*

*cessing.*")]

**Regarding Claim 46:**

*Gopinathan et al.* teaches,

A system as claimed in claim 1 wherein the interaction data includes the date and/or time of the interaction and wherein the neural network is trained on data including the date and/or time of the interaction. **[FIG. 4; (col. 4, line 13-19 "***FIG. 4 shows transaction analysis screen 401 that allows the fraud analyst to examine each high-risk transaction and determine appropriate fraud control actions. It includes account information 402, fraud score 403, explanations derived from reason codes 404 that indicate the reasons for fraud score 403,* ***and two scrolling windows 405 and 406 that show transaction information for the current day and the past seven days 405, and for the past six months 406.***")]

**Regarding Claim 47:**

*Gopinathan et al.* teaches,

A system as claimed in claim 1 wherein one or more of the merchants operate from one or more commercial premises, the interaction data includes a monetary value of the interaction and wherein the neural network is trained on data including the monetary value of the interaction. **[FIG. 1 & FIG. 4; ("***Referring now to FIG. 1, there is shown a block diagram of a typical implementation of a system 100 in accordance with the present invention.* ***Transaction information is applied to system 100 via data network 105, which is connected to a conventional financial***

***data facility 106 collecting transaction information from conventional sources such as human-operated credit-card authorization terminals and automated teller machines (not shown).*** *CPU 101 runs software program instructions, stored in program storage 107, which direct CPU 101 to perform the various functions of the system.*") **& (col. 4, line 13-19 "***FIG. 4** shows transaction analysis screen 401 that allows the fraud analyst to examine each high-risk transaction and determine appropriate fraud control actions. It includes account information 402, fraud score 403, explanations derived from reason codes 404 that indicate the reasons for fraud score 403,* ***and two scrolling windows 405 and 406 that show transaction information for the current day and the past seven days 405, and for the past six months 406.***")]

**Regarding Claim 52:**

*Gopinathan et al.* teaches,

A neural network training system comprising:

a memory in which is maintained an interaction database of interaction data representing interactions between customers and merchants; **[FIG. 1 & FIG. 4; (col. 3, line 47-65 "***In accordance with the software program instructions, CPU 101 stores the data obtained from data network 105 in data storage 103, and uses RAM 102 in a conventional manner as a workspace. CPU 101, data storage 103, and program storage 107 operate together to provide a neural network model 108 for predicting fraud. After neural network 108 processes the information, as described below, to obtain an indication of the likelihood of fraud, a signal indicative of that likelihood is sent from CPU 101 to output device 104.* ***In the preferred embodiment, CPU 101 is***

***a Model 3090 IBM mainframe computer, RAM 102 and data storage 103 are conventional RAM, ROM and disk storage devices for the Model 3090 CPU, and output device 104 is a conventional means for either printing results based on the signals generated by neural network 108, or displaying the results on a video screen using a window-based interface system, or sending the results to a database for later access, or sending a signal dependent on the results to an authorization system (not shown) for further processing.*****"**) **&** **(col. 5, line 54 to col. 6, line 6 "***Neural networks learn from examples by modifying their weights. The "training" process, the general techniques of which are well known in the art, involves the following steps: 1) Repeatedly presenting examples of a particular input/output task to the neural network model; 2) Comparing the model output and desired output to measure error; and 3) Modifying model weights to reduce the error. This set of steps is repeated until further iteration fails to decrease the error. Then, the network is said to be "trained."* ***Once training is completed, the network can predict outcomes for new data inputs.*** *Fraud-Related Variables:* ***In the present invention, data used to train the model are drawn from various database files containing historical data on individual transactions, merchants, and customers. These data are preferably pre-processed before being fed into the neural network, resulting in the creation of a set of fraud-related variables that have been empirically determined to form more effective predictors of fraud than the original historical data.*****")]**

a retrieval device arranged to retrieve from the interaction database data representing interactions between customers and merchants; **[FIG. 1 & FIG. 4; (col. 3, line 47-55 "***In accordance with the software program instructions, CPU 101 stores the data obtained from data network 105 in data storage 103, and uses RAM 102 in a conventional manner as a workspace. CPU 101, data*

***storage 103, and program storage 107 operate together to provide a neural network model 108 for predicting fraud.*** *After neural network 108 processes the information, as described below, to obtain an indication of the likelihood of fraud, a signal indicative of that likelihood is sent from CPU 101 to output device 104.*") **& (col. 5, line 54 to col. 6, line 6** "*Neural networks learn from examples by modifying their weights. The "training" process, the general techniques of which are well known in the art, involves the following steps: 1) Repeatedly presenting examples of a particular input/output task to the neural network model; 2) Comparing the model output and desired output to measure error; and 3) Modifying model weights to reduce the error. This set of steps is repeated until further iteration fails to decrease the error. Then, the network is said to be "trained."* ***Once training is completed, the network can predict outcomes for new data inputs.*** *Fraud-Related Variables:* ***In the present invention, data used to train the model are drawn from various database files containing historical data on individual transactions, merchants, and customers. These data are preferably pre-processed before being fed into the neural network, resulting in the creation of a set of fraud-related variables that have been empirically determined to form more effective predictors of fraud than the original historical data.***")]

a neural network arranged to receive input data representing the data retrieved from the interaction database and to output prediction data representing interaction data predicted by the neural network; **[FIG. 1; (col. 3, line 47-55** "*In accordance with the software program instructions, CPU 101 stores the data obtained from data network 105 in data storage 103, and uses RAM 102 in a conventional manner as a workspace.* ***CPU 101, data storage 103, and program storage 107 operate together to provide a neural network model 108 for predicting fraud.*** *After neural network 108 processes the information, as described below, to obtain an indication of the*

*likelihood of fraud, a signal indicative of that likelihood is sent from CPU 101 to output device 104.*") and

a training device arranged to compare the data retrieved from the interaction database and the prediction data and to adjust the neural network based on the comparison. **[(col. 5, line 54 to col. 6, line 6** "*Neural networks learn from examples by modifying their weights. The "training" process, the general techniques of which are well known in the art, involves the following steps: 1) Repeatedly presenting examples of a particular input/output task to the neural network model; 2)* ***Comparing*** *the model output and desired output to measure error; and 3)* ***Modifying*** *model weights to reduce the error. This set of steps is repeated until further iteration fails to decrease the error. Then, the network is said to be "****trained.****" **Once training is completed, the network can predict outcomes for new data inputs**. Fraud-Related Variables: **In the present invention, data used to train the model are drawn from various database files containing historical data on individual transactions, merchants, and customers. These data are preferably pre-processed before being fed into the neural network, resulting in the creation of a set of fraud-related variables that have been empirically determined to form more effective predictors of fraud than the original historical data.**")]

**Regarding Claim 53:**

*Gopinathan et al.* teaches,

A neural network training system as claimed in claim 52 wherein the interaction data includes the date and/or time of the interaction, the neural network further arranged to receive as input the

date and/or time of interactions between customers and merchants. **[FIG. 4; (col. 4, line 13-19** "*FIG. 4 shows transaction analysis screen 401 that allows the fraud analyst to examine each high-risk transaction and determine appropriate fraud control actions. It includes account information 402, fraud score 403, explanations derived from reason codes 404 that indicate the reasons for fraud score 403,* ***and two scrolling windows 405 and 406 that show transaction information for the current day and the past seven days 405, and for the past six months 406.***")]

**Regarding Claim 54:**

*Gopinathan et al.* teaches,

A neural network training system as claimed in claim 52 wherein one or more merchants operates from one or more commercial premises, the interaction data includes a monetary value of the interaction and wherein the neural network is further arranged to receive as input the monetary value of the interaction. **[FIG. 1 & FIG. 4; ("***Referring now to FIG. 1, there is shown a block diagram of a typical implementation of a system 100 in accordance with the present invention.* ***Transaction information is applied to system 100 via data network 105, which is connected to a conventional financial data facility 106 collecting transaction information from conventional sources such as human-operated credit-card authorization terminals and automated teller machines (not shown).*** *CPU 101 runs software program instructions, stored in program storage 107, which direct CPU 101 to perform the various functions of the system.*") **& (col. 4, line 13-19** "*FIG. 4 shows transaction analysis screen 401 that allows the fraud analyst to examine each high-risk transaction and determine appropriate fraud control actions. It includes*

*account information 402, fraud score 403, explanations derived from reason codes 404 that indicate the reasons for fraud score 403,* ***and two scrolling windows 405 and 406 that show transaction information for the current day and the past seven days 405, and for the past six months 406.")]***

**Regarding Claim 59:**

*Gopinathan et al.* teaches,

An interaction prediction computer program comprising:

a neural network maintained in a memory, the neural network trained on data retrieved from an interaction database of interaction data representing interactions between customers and merchants; **[FIG. 1 & FIG. 4; (col. 3, line 47-65 "*In accordance with the software program instructions, CPU 101 stores the data obtained from data network 105 in data storage 103, and uses RAM 102 in a conventional manner as a workspace. CPU 101, data storage 103, and program storage 107 operate together to provide a neural network model 108 for predicting fraud.* *After neural network 108 processes the information, as described below, to obtain an indication of the likelihood of fraud, a signal indicative of that likelihood is sent from CPU 101 to output device 104.* ***In the preferred embodiment, CPU 101 is a Model 3090 IBM mainframe computer, RAM 102 and data storage 103 are conventional RAM, ROM and disk storage devices for the Model 3090 CPU, and output device 104 is a conventional means for either printing results based on the signals generated by neural network 108, or displaying the results on a video screen using a window-based interface system, or sending the results to a***

***database for later access, or sending a signal dependent on the results to an authorization system (not shown) for further processing.***") & **(col. 5, line 54 to col. 6, line 6** "*Neural networks learn from examples by modifying their weights. The "training" process, the general techniques of which are well known in the art, involves the following steps: 1) Repeatedly presenting examples of a particular input/output task to the neural network model; 2) Comparing the model output and desired output to measure error; and 3) Modifying model weights to reduce the error. This set of steps is repeated until further iteration fails to decrease the error. Then, the network is said to be "trained."* ***Once training is completed, the network can predict outcomes for new data inputs.*** *Fraud-Related Variables:* ***In the present invention, data used to train the model are drawn from various database files containing historical data on individual transactions, merchants, and customers. These data are preferably pre-processed before being fed into the neural network, resulting in the creation of a set of fraud-related variables that have been empirically determined to form more effective predictors of fraud than the original historical data.***")]

a retrieval device arranged to activate the neural network and to retrieve prediction data representing future interactions between customers and merchants; **[FIG. 1 & FIG. 4; (col. 3, line 47-55** "***In accordance with the software program instructions, CPU 101 stores the data obtained from data network 105 in data storage 103, and uses RAM 102 in a conventional manner as a workspace. CPU 101, data storage 103, and program storage 107 operate together to provide a neural network model 108 for predicting fraud.*** *After neural network 108 processes the information, as described below, to obtain an indication of the likelihood of fraud, a signal indicative of that likelihood is sent from CPU 101 to output device 104.*") & **(col. 5,**

**line 54 to col. 6, line 6** "*Neural networks learn from examples by modifying their weights. The "training" process, the general techniques of which are well known in the art, involves the following steps: 1) Repeatedly presenting examples of a particular input/output task to the neural network model; 2) Comparing the model output and desired output to measure error; and 3) Modifying model weights to reduce the error. This set of steps is repeated until further iteration fails to decrease the error. Then, the network is said to be "trained."* ***Once training is completed, the network can predict outcomes for new data inputs.*** *Fraud-Related Variables:* ***In the present invention, data used to train the model are drawn from various database files containing historical data on individual transactions, merchants, and customers. These data are preferably pre-processed before being fed into the neural network, resulting in the creation of a set of fraud-related variables that have been empirically determined to form more effective predictors of fraud than the original historical data.***")] and

a display arranged to display a representation of the prediction data. **[(col. 3, line 56-65** "*In the preferred embodiment, CPU 101 is a Model 3090 IBM mainframe computer, RAM 102 and data storage 103 are conventional RAM, ROM and disk storage devices for the Model 3090 CPU, and output device 104 is a conventional means for either printing results based on the signals generated by neural network 108, or* ***displaying the results on a video screen using a window-based interface system****, or sending the results to a database for later access, or sending a signal dependent on the results to an authorization system (not shown) for further processing.*")]

**Regarding Claim 60:**

*Gopinathan et al.* teaches,

A computer program as claimed in claim 59 wherein the interaction data includes the date and/or time of the interaction and wherein the neural network is trained on data including the date and/or time of the interaction. **[FIG. 4; (col. 4, line 13-19 "***FIG. 4 shows transaction analysis screen 401 that allows the fraud analyst to examine each high-risk transaction and determine appropriate fraud control actions. It includes account information 402, fraud score 403, explanations derived from reason codes 404 that indicate the reasons for fraud score 403,* ***and two scrolling windows 405 and 406 that show transaction information for the current day and the past seven days 405, and for the past six months 406.*****")]**

**Regarding Claim 61:**

*Gopinathan et al.* teaches,

A computer program as claimed in claim 59 wherein one or more of the merchants operate from one or more commercial premises, the interaction data includes a monetary value of the interaction and wherein the neural network is trained on data including the monetary value of the interaction. **[FIG. 1 & FIG. 4; ("***Referring now to FIG. 1, there is shown a block diagram of a typical implementation of a system 100 in accordance with the present invention.* ***Transaction information is applied to system 100 via data network 105, which is connected to a conventional financial data facility 106 collecting transaction information from conventional sources such as human-operated credit-card authorization terminals and automated teller machines (not shown).*** *CPU 101 runs software program instructions, stored in program storage*

*107, which direct CPU 101 to perform the various functions of the system.*") & **(col. 4, line 13-19** "*FIG. 4 shows transaction analysis screen 401 that allows the fraud analyst to examine each high-risk transaction and determine appropriate fraud control actions. It includes account information 402, fraud score 403, explanations derived from reason codes 404 that indicate the reasons for fraud score 403,* ***and two scrolling windows 405 and 406 that show transaction information for the current day and the past seven days 405, and for the past six months 406.***")]

**Regarding Claim 66:**

*Gopinathan et al.* teaches,

A computer program as claimed in claim 59 embodied on a computer readable medium.

**[FIG. 1; (col. 3, line 44-46** "*In the preferred embodiment, the software program is written in the ANSI C language, which may be run on a variety of conventional hardware platforms.*")]

**Regarding Claim 67:**

*Gopinathan et al.* teaches,

A neural network training computer program comprising:

an interaction database of interaction data representing interactions between customers and merchants maintained in a memory; **[FIG. 1 & FIG. 4; (col. 3, line 47-65** "***In accordance with the software program instructions, CPU 101 stores the data obtained from data network 105 in***

***data storage 103, and uses RAM 102 in a conventional manner as a workspace. CPU 101, data storage 103, and program storage 107 operate together to provide a neural network model 108 for predicting fraud.*** *After neural network 108 processes the information, as described below, to obtain an indication of the likelihood of fraud, a signal indicative of that likelihood is sent from CPU 101 to output device 104.* ***In the preferred embodiment, CPU 101 is a Model 3090 IBM mainframe computer, RAM 102 and data storage 103 are conventional RAM, ROM and disk storage devices for the Model 3090 CPU, and output device 104 is a conventional means for either printing results based on the signals generated by neural network 108, or displaying the results on a video screen using a window-based interface system, or sending the results to a database for later access, or sending a signal dependent on the results to an authorization system (not shown) for further processing.***") **& (col. 5, line 54 to col. 6, line 6 "***Neural networks learn from examples by modifying their weights. The "training" process, the general techniques of which are well known in the art, involves the following steps: 1) Repeatedly presenting examples of a particular input/output task to the neural network model; 2) Comparing the model output and desired output to measure error; and 3) Modifying model weights to reduce the error. This set of steps is repeated until further iteration fails to decrease the error. Then, the network is said to be "trained."* ***Once training is completed, the network can predict outcomes for new data inputs.*** *Fraud-Related Variables:* ***In the present invention, data used to train the model are drawn from various database files containing historical data on individual transactions, merchants, and customers. These data are preferably pre-processed before being fed into the neural network, resulting in the creation of a set of fraud-related variables that have been empirically determined to form more effective predictors of***

***fraud than the original historical data.")]***

a retrieval device arranged to retrieve from the interaction database data representing interactions between customers and merchants; **[FIG. 1 & FIG. 4; (col. 3, line 47-55 "*In accordance with the software program instructions, CPU 101 stores the data obtained from data network 105 in data storage 103, and uses RAM 102 in a conventional manner as a workspace. CPU 101, data storage 103, and program storage 107 operate together to provide a neural network model 108 for predicting fraud. After neural network 108 processes the information, as described below, to obtain an indication of the likelihood of fraud, a signal indicative of that likelihood is sent from CPU 101 to output device 104.*") & (col. 5, line 54 to col. 6, line 6** "*Neural networks learn from ]examples by modifying their weights. The "training" process, the general techniques of which are well known in the art, involves the following steps: 1) Repeatedly presenting examples of a particular input/output task to the neural network model; 2) Comparing the model output and desired output to measure error; and 3) Modifying model weights to reduce the error. This set of steps is repeated until further iteration fails to decrease the error. Then, the network is said to be "trained."* ***Once training is completed, the network can predict outcomes for new data inputs.*** *Fraud-Related Variables:* ***In the present invention, data used to train the model are drawn from various database files containing historical data on individual transactions, merchants, and customers. These data are preferably pre-processed before being fed into the neural network, resulting in the creation of a set of fraud-related variables that have been empirically determined to form more effective predictors of fraud than the original historical data.")]***

a neural network maintained in a memory, the neural network arranged to receive input data

representing the data retrieved from the interaction database and to output prediction data representing interaction data predicted by the neural network; **[FIG. 1; (col. 3, line 47-65 "*In accordance with the software program instructions, CPU 101 stores the data obtained from data network 105 in data storage 103, and uses RAM 102 in a conventional manner as a workspace. CPU 101, data storage 103, and program storage 107 operate together to provide a neural network model 108 for predicting fraud.*")]** and

a training device arranged to compare the data retrieved from the interaction database and the prediction data and to adjust the neural network based on the comparison. **[(col. 5, line 54 to col. 6, line 6 "***Neural networks learn from ]examples by modifying their weights. The "training" process, the general techniques of which are well known in the art, involves the following steps: 1) Repeatedly presenting examples of a particular input/output task to the neural network model; 2) Comparing the model output and desired output to measure error; and 3) Modifying model weights to reduce the error. This set of steps is repeated until further iteration fails to decrease the error. Then, the network is said to be "trained." **Once training is completed, the network can predict outcomes for new data inputs**. Fraud-Related Variables: **In the present invention, data used to train the model are drawn from various database files containing historical data on individual transactions, merchants, and customers. These data are preferably pre-processed before being fed into the neural network, resulting in the creation of a set of fraud-related variables that have been empirically determined to form more effective predictors of fraud than the original historical data.***")]**

**Regarding Claim 68:**

*Gopinathan et al.* teaches,

A computer program as claimed in claim 67 wherein the interaction data includes the date and/or time of the interaction, the neural network further arranged to receive as input the date and/or time of interactions between customers and merchants. **[FIG. 4; (col. 4, line 13-19 "***FIG. 4 shows transaction analysis screen 401 that allows the fraud analyst to examine each high-risk transaction and determine appropriate fraud control actions. It includes account information 402, fraud score 403, explanations derived from reason codes 404 that indicate the reasons for fraud score 403,* ***and two scrolling windows 405 and 406 that show transaction information for the current day and the past seven days 405, and for the past six months 406.*****")]**

**Regarding Claim 69:**

*Gopinathan et al.* teaches,

A computer program as claimed in claim 67 wherein one or more merchants operates from one or more commercial premises, the interaction data includes the monetary value of the interaction and wherein the neural network is trained on data including the monetary value of the interaction. **[FIG. 1 & FIG. 4; ("***Referring now to FIG. 1, there is shown a block diagram of a typical implementation of a system 100 in accordance with the present invention.* ***Transaction information is applied to system 100 via data network 105, which is connected to a conventional financial data facility 106 collecting transaction information from conventional sources such as human-operated credit-card authorization terminals and automated teller machines (not shown).*** *CPU 101 runs software program instructions, stored in program storage*

*107, which direct CPU 101 to perform the various functions of the system.*") **& (col. 4, line 13-19** "*FIG. 4 shows transaction analysis screen 401 that allows the fraud analyst to examine each high-risk transaction and determine appropriate fraud control actions. It includes account information 402, fraud score 403, explanations derived from reason codes 404 that indicate the reasons for fraud score 403,* ***and two scrolling windows 405 and 406 that show transaction information for the current day and the past seven days 405, and for the past six months 406.***")]

**Regarding Claim 74:**

*Gopinathan et al.* teaches,

A computer program as claimed in claim 67 embodied on a computer readable medium. **[FIG. 1; (col. 3, line 44-46** "*In the preferred embodiment, the software program is written in the ANSI C language, which may be run on a variety of conventional hardware platforms.*")]

**Regarding Claim 75:**

*Gopinathan et al.* teaches,

A method of predicting interactions between customers and merchants, the method comprising the steps of:

maintaining in a memory a neural network trained on data retrieved on an interaction database of interaction data representing interactions between customers and merchants; **[FIG. 1 & FIG.**

**4; (col. 3, line 47-65 "*In accordance with the software program instructions, CPU 101 stores the data obtained from data network 105 in data storage 103, and uses RAM 102 in a conventional manner as a workspace. CPU 101, data storage 103, and program storage 107 operate together to provide a neural network model 108 for predicting fraud.* *After neural network 108 processes the information, as described below, to obtain an indication of the likelihood of fraud, a signal indicative of that likelihood is sent from CPU 101 to output device 104.* *In the preferred embodiment, CPU 101 is a Model 3090 IBM mainframe computer, RAM 102 and data storage 103 are conventional RAM, ROM and disk storage devices for the Model 3090 CPU, and output device 104 is a conventional means for either printing results based on the signals generated by neural network 108, or displaying the results on a video screen using a window-based interface system, or sending the results to a database for later access, or sending a signal dependent on the results to an authorization system (not shown) for further processing.*") & (col. 5, line 54 to col. 6, line 6 "*Neural networks learn from examples by modifying their weights. The "training" process, the general techniques of which are well known in the art, involves the following steps: 1) Repeatedly presenting examples of a particular input/output task to the neural network model; 2) Comparing the model output and desired output to measure error; and 3) Modifying model weights to reduce the error. This set of steps is repeated until further iteration fails to decrease the error. Then, the network is said to be "trained."* *Once training is completed, the network can predict outcomes for new data inputs.* *Fraud-Related Variables:* *In the present invention, data used to train the model are drawn from various database files containing historical data on individual transactions, merchants, and customers. These data are preferably pre-processed before being fed into the neural*

***network, resulting in the creation of a set of fraud-related variables that have been empirically determined to form more effective predictors of fraud than the original historical data.")]***

activating the neural network; **[FIG. 11; (col. 6, line 05-17 "***Referring now to FIG. 11, there is shown a* ***flowchart of the pre-processing method of the present invention****. Individual elements of the flowchart are indicated by designations which correspond to module names. The following brief description summarizes the processing. Data used for pre-processing is taken from three databases which contain past data: 1) past transaction database 1101 (also called an "authorization database") containing two years' worth of past transaction data, which may be implemented in the same data base as past data 804; 2) customer database 1103 containing customer data; and 3) fraud database 1102 which indicates which accounts had fraudulent activity and when the fraudulent activity occurred.***") & (col. 7, line 18-21 "***The result is called the mod1n2 data set 1121 (also called the "training set"), which contains the fraud-related variables needed to train the network.***")]**

retrieving prediction data representing future interactions between customers and merchants from the neural network; **[FIG. 1 & FIG. 4; (col. 3, line 47-55 "*In accordance with the software program instructions, CPU 101 stores the data obtained from data network 105 in data storage 103, and uses RAM 102 in a conventional manner as a workspace. CPU 101, data storage 103, and program storage 107 operate together to provide a* neural network *model 108 for* predicting *fraud. After* neural network *108 processes the information, as described below, to obtain an indication of the likelihood of fraud, a signal indicative of that likelihood is sent from CPU 101 to output device 104.*") & (col. 5, line 54 to col. 6, line 6 "***Neural networks learn from examples by modifying their weights. The "training" process, the general techniques of which are well***

*known in the art, involves the following steps: 1) Repeatedly presenting examples of a particular input/output task to the neural network model; 2) Comparing the model output and desired output to measure error; and 3) Modifying model weights to reduce the error. This set of steps is repeated until further iteration fails to decrease the error. Then, the network is said to be "trained."* ***Once training is completed, the network can predict outcomes for new data inputs.*** *Fraud-Related Variables:* ***In the present invention, data used to train the model are drawn from various database files containing historical data on individual transactions, merchants, and customers. These data are preferably pre-processed before being fed into the neural network, resulting in the creation of a set of fraud-related variables that have been empirically determined to form more effective predictors of fraud than the original historical data.")]*** and displaying a representation of the prediction data. **[(col. 3, line 56-65 "***In the preferred embodiment, CPU 101 is a Model 3090 IBM mainframe computer, RAM 102 and data storage 103 are conventional RAM, ROM and disk storage devices for the Model 3090 CPU, and output device 104 is a conventional means for either printing results based on the signals generated by neural network 108, or* ***displaying the results on a video screen using a window-based interface system****, or sending the results to a database for later access, or sending a signal dependent on the results to an authorization system (not shown) for further processing.")]**

**Regarding Claim 76:**

*Gopinathan et al.* teaches,

A method as claimed in claim 75 wherein the interaction data includes the date and/or time of the

interaction and wherein the neural network is trained on data including the date and/or time of the interaction. **[FIG. 4; (col. 4, line 13-19 "***FIG. 4 shows transaction analysis screen 401 that allows the fraud analyst to examine each high-risk transaction and determine appropriate fraud control actions. It includes account information 402, fraud score 403, explanations derived from reason codes 404 that indicate the reasons for fraud score 403,* ***and two scrolling windows 405 and 406 that show transaction information for the current day and the past seven days 405, and for the past six months 406.*****")]**

**Regarding Claim 77:**

*Gopinathan et al.* teaches,

A method as claimed in claim 75 wherein one or more of the merchants operate from one or more commercial premises, the interaction data includes the monetary value of the interaction and wherein the neural network is trained on data including the monetary value of the interaction. **[FIG. 1 & FIG. 4; ("***Referring now to FIG. 1, there is shown a block diagram of a typical implementation of a system 100 in accordance with the present invention.* ***Transaction information is applied to system 100 via data network 105, which is connected to a conventional financial data facility 106 collecting transaction information from conventional sources such as human-operated credit-card authorization terminals and automated teller machines (not shown).*** *CPU 101 runs software program instructions, stored in program storage 107, which direct CPU 101 to perform the various functions of the system.*") & (col. 4, line 13-19 "*FIG. 4 shows transaction analysis screen 401 that allows the fraud analyst to examine each high-risk transaction and determine appropriate fraud control actions. It includes account*

*information 402, fraud score 403, explanations derived from reason codes 404 that indicate the reasons for fraud score 403,* ***and two scrolling windows 405 and 406 that show transaction information for the current day and the past seven days 405, and for the past six months 406.*****")]**

**Regarding Claim 82:**

*Gopinathan et al.* teaches,

A method of training a neural network comprising the steps of:

maintaining in a memory an interaction database of interaction data representing interactions between customers and merchants; **[FIG. 1 & FIG. 4; (col. 3, line 47-65 "*In accordance with the software program instructions, CPU 101 stores the data obtained from data network 105 in data storage 103, and uses RAM 102 in a conventional manner as a workspace. CPU 101, data storage 103, and program storage 107 operate together to provide a neural network model 108 for predicting fraud. After neural network 108 processes the information, as described below, to obtain an indication of the likelihood of fraud, a signal indicative of that likelihood is sent from CPU 101 to output device 104. In the preferred embodiment, CPU 101 is a Model 3090 IBM mainframe computer, RAM 102 and data storage 103 are conventional RAM, ROM and disk storage devices for the Model 3090 CPU, and output device 104 is a conventional means for either printing results based on the signals generated by neural network 108, or displaying the results on a video screen using a window-based interface system, or sending the results to a database for later access, or sending a signal dependent on the results to an authorization*

***system (not shown) for further processing.***") & (col. 5, line 54 to col. 6, line 6 "*Neural networks learn from examples by modifying their weights. The "training" process, the general techniques of which are well known in the art, involves the following steps: 1) Repeatedly presenting examples of a particular input/output task to the neural network model; 2) Comparing the model output and desired output to measure error; and 3) Modifying model weights to reduce the error. This set of steps is repeated until further iteration fails to decrease the error. Then, the network is said to be "trained."* ***Once training is completed, the network can predict outcomes for new data inputs.*** *Fraud-Related Variables:* ***In the present invention, data used to train the model are drawn from various database files containing historical data on individual transactions, merchants, and customers. These data are preferably pre-processed before being fed into the neural network, resulting in the creation of a set of fraud-related variables that have been empirically determined to form more effective predictors of fraud than the original historical data.***")]

retrieving from the interaction database data representing interactions between customers and merchants; [**FIG. 1 & FIG. 4; (col. 3, line 47-55 "*In accordance with the software program instructions, CPU 101 stores the data obtained from data network 105 in data storage 103, and uses RAM 102 in a conventional manner as a workspace. CPU 101, data storage 103, and program storage 107 operate together to provide a neural network model 108 for predicting fraud.* *After neural network 108 processes the information, as described below, to obtain an indication of the likelihood of fraud, a signal indicative of that likelihood is sent from CPU 101 to output device 104.*")]

arranging a neural network to receive input data representing the data retrieved from the

interaction database and to output prediction data representing interaction data predicted by the neural network; **[(col. 5, line 64 to col. 6, line 04 " *In the present invention, data used to train the model are drawn from various database files containing historical data on individual transactions, merchants, and customers. These data are preferably pre-processed before being fed into the neural network, resulting in the creation of a set of fraud-related variables that have been empirically determined to form more effective predictors of fraud than the original historical data.*")]** and

comparing the data retrieved from the interaction database and the prediction data and adjusting the neural network based on the comparison. **[(col. 5, line 54 to col. 6, line 6 "***Neural networks learn from examples by modifying their weights. The "training" process, the general techniques of which are well known in the art, involves the following steps: 1) Repeatedly presenting examples of a particular input/output task to the neural network model; 2) Comparing the model output and desired output to measure error; and 3) Modifying model weights to reduce the error. This set of steps is repeated until further iteration fails to decrease the error. Then, the network is said to be "trained." **Once training is completed, the network can predict outcomes for new data inputs.** Fraud-Related Variables: **In the present invention, data used to train the model are drawn from various database files containing historical data on individual transactions, merchants, and customers. These data are preferably pre-processed before being fed into the neural network, resulting in the creation of a set of fraud-related variables that have been empirically determined to form more effective predictors of fraud than the original historical data.**")]**

**Regarding Claim 83:**

*Gopinathan et al.* teaches,

A method of training a neural network as claimed in claim 82 wherein the interaction data includes the date and/or time of the interaction, the method comprising the step of arranging the neural network to receive as input the date and/or time of interactions between customers and merchants. **[FIG. 4; (col. 4, line 13-19 "***FIG. 4 shows transaction analysis screen 401 that allows the fraud analyst to examine each high-risk transaction and determine appropriate fraud control actions. It includes account information 402, fraud score 403, explanations derived from reason codes 404 that indicate the reasons for fraud score 403,* ***and two scrolling windows 405 and 406 that show transaction information for the current day and the past seven days 405, and for the past six months 406.*****")]**

**Regarding Claim 84:**

*Gopinathan et al.* teaches,

A method of training a neural network as claimed in claim 82 wherein one or more merchants operates from one or more commercial premises and the interaction data includes the monetary value of the interaction, the method further comprising the step of arranging the neural network to receive as input the monetary value of the interaction. **[FIG. 1 & FIG. 4; ("***Referring now to FIG. 1, there is shown a block diagram of a typical implementation of a system 100 in accordance with the present invention.* ***Transaction information is applied to system 100 via data network 105, which is connected to a conventional financial data facility 106 collecting transaction information from conventional sources such as human-operated credit-card***

***authorization terminals and automated teller machines (not shown).*** *CPU 101 runs software program instructions, stored in program storage 107, which direct CPU 101 to perform the various functions of the system.*") **& (col. 4, line 13-19** "*FIG. 4 shows transaction analysis screen 401 that allows the fraud analyst to examine each high-risk transaction and determine appropriate fraud control actions. It includes account information 402, fraud score 403, explanations derived from reason codes 404 that indicate the reasons for fraud score 403,* ***and two scrolling windows 405 and 406 that show transaction information for the current day and the past seven days 405, and for the past six months 406.***")]

**Regarding Claim 89:**

*Gopinathan et al.* teaches,

A neural network trained by the method as claimed in claim 82. **[(col. 5, line 54 to col. 6, line 6** "*Neural networks learn from examples by modifying their weights. The "training" process, the general techniques of which are well known in the art, involves the following steps: 1) Repeatedly presenting examples of a particular input/output task to the neural network model; 2) Comparing the model output and desired output to measure error; and 3) Modifying model weights to reduce the error. This set of steps is repeated until further iteration fails to decrease the error. Then, the network is said to be "trained."* ***Once training is completed, the network can predict outcomes for new data inputs.*** *Fraud-Related Variables:* ***In the present invention, data used to train the model are drawn from various database files containing historical data on individual transactions, merchants, and customers. These data are preferably pre-***

***processed before being fed into the neural network, resulting in the creation of a set of fraud-related variables that have been empirically determined to form more effective predictors of fraud than the original historical data.*")]**

# Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. **Claims 48-51, 55-58, 62-65, 70-73, 78-81 & 85-88** are rejected under 35 U.S.C. 103(a) as being unpatentable over

**Gopinathan et al. (USPN 5,819,226), Filed: Sep. 08, 1992; Date of Patent: Oct. 06, 1998,**

in view of

**LeStrange et al. (USPN 5,470,079), Filed: Jun. 16,1994; Date of Patent: Nov. 28, 1995.**

The *Gopinathan et al.* reference has been discussed above and does not explicitly teach the limitations of **claims 48-51, 55-58, 62-65, 70-73, 78-81 & 85-88**. However *LeStrange et al.* teaches the limitations of **claims 48-51, 55-58, 62-65, 70-73, 78-81 & 85-88**.

**Regarding Claim 48, 55, 62, 70, 78 & 85:**

*LeStrange et al.* teaches,

A system as claimed in claim 47 wherein one or more of the merchants operates a casino or gaming venue comprising one or more gaming machines, each gaming machine having a machine identifier. **[FIG. 2; (col. 5, lines 47-67 "***FIG. 2 shows a schematic block diagram of the game accounting system for use in connection with the present invention.* ***Accounting system***

***comprises a plurality of accounting meters 34, which includes a set of drop meters 38 and game activity meters 36, for tracing all money flows and game activity, respectively, for the particular machine.*** *The accounting meters 34 are non-reset, accumulative meters and thus they establish an audit trail for the various quantities they track. In addition, credit meters 28 monitor game credit and provide separate meters for the total game credit available to the player and the amount of that credit that has not yet been risked. The accounting system also includes a game event processor 26, which responds to a variety of gaming machine events and updates the accounting meters accordingly. The event processor 26 is compatible with a variety of gaming machines, including traditional coin-only machines as well as the more advanced automated cashless versions.* ***The accounting meters 34 provide a complete record of all gaming activity at the gaming machine.***"**)]** It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matters pertains to combine the references. Because, the uniqueness of the individual accounting transactions constitutes a way for tracing all financial and gaming transactions down the individual machine. Moreover, the ability to track the individual transactions (e.g., down to the actual date, time and machine location), assists businesses forecast and expand, monitor customer trends and spending habits, monitor fraudulent transactions, service and maintain the individual machines, etc.

**Regarding Claim 49, 56, 63, 71, 79 & 86:**

*LeStrange et al.* teaches,

A system as claimed in claim 48 wherein the interaction data includes a machine identifier for each interaction and wherein the neural network (as taught by *Gopinathan et al.*) is trained on data including the machine identifier for interactions between customers and merchants.

**[FIG. 2; (col. 5, lines 47-67 "***FIG. 2 shows a schematic block diagram of the game accounting system for use in connection with the present invention.* ***Accounting system comprises a plurality of accounting meters 34, which includes a set of drop meters 38 and game activity meters 36, for tracing all money flows and game activity, respectively, for the particular machine.*** *The accounting meters 34 are non-reset, accumulative meters and thus they establish an audit trail for the various quantities they track. In addition, credit meters 28 monitor game credit and provide separate meters for the total game credit available to the player and the amount of that credit that has not yet been risked. The accounting system also includes a game event processor 26, which responds to a variety of gaming machine events and updates the accounting meters accordingly. The event processor 26 is compatible with a variety of gaming machines, including traditional coin-only machines as well as the more advanced automated cashless versions.* ***The accounting meters 34 provide a complete record of all gaming activity at the gaming machine.***"**)]** It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matters pertains, to include a machine identifier with the information being fed to the neural network. Note, the neural network retains all the weights from the training programming. When the system information is input into

the neural network. The neural network can better predict all transaction processing right down to the individual machines.

**Regarding Claim 50, 57, 64, 72, 80 & 87:**

*LeStrange et al.* teaches,

A system as claimed in claim 48 wherein each gaming machine has a spatial position, the interaction data includes the spatial position of the machine involved in the interaction and wherein the neural network (as taught by *Gopinathan et al.*) is trained on data including the spatial position of the machine involved in the interaction. **[(col. 3, line 65 to col. 4, line 03** "*Furthermore, when the system transmits data to other components within the system, it transmits both accounting and event data in a single message. Therefore,* ***a host computer system can log the data to a database while maintaining the proper relationship between the data and the corresponding state of the gaming machine.***") **& (col. 5, line 06-14** "*As shown in FIG. 1, in the preferred embodiment the primary hardware elements of the system include a game monitor unit (GMU) 16, a computer network interface 18, and a central or host computer system 20. The game monitor unit 16 collects information from gaming machine 10 and performs game accounting and other monitoring and security functions.* ***GMU 16 transmits accounting data along with information about the current state of gaming machine 10 to the host computer 20 via the network interface 18.***")] It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matters pertains, to include in the system log data to the database, spatial positioning i.e., the geographical locations of the individual gaming machines e.g., casinos offer various promotions and sweepstakes throughout

the day. The proximity of gaming machines by front and rear entrances juxtaposed between middle isles, allow casinos and merchants to capitalize on different customers habits or impulsive desires. Moreover, the proximity, to other gaming and gambling events allows them to further capitalize on different customers wants and needs. The inclusion of such data pertaining to the different geographical location of different gaming machines, allows casino owners and merchants to further monitor and predict customer habits and gaming desire, as well as add to their own bottom-line.

**Regarding Claim 51, 58, 65, 73, 81 & 88:**

*LeStrange et al.* teaches,

A system as claimed in claim 50 wherein the neural network (as taught by *Gopinathan et al.*) is trained on data including the machine identifier and/or spatial position of machines neighboring each machine involved in interactions between customers and merchants. **[(col. 3, line 65 to col. 4, line 03 "***Furthermore, when the system transmits data to other components within the system, it transmits both accounting and event data in a single message. Therefore,* ***a host computer system can log the data to a database while maintaining the proper relationship between the data and the corresponding state of the gaming machine.*****") & (col. 5, line 06-14 "***As shown in FIG. 1, in the preferred embodiment the primary hardware elements of the system include a game monitor unit (GMU) 16, a computer network interface 18, and a central or host computer system 20. The game monitor unit 16 collects information from gaming machine 10 and performs game accounting and other monitoring and security functions.* ***GMU 16 transmits accounting data along with information about the current state of gaming machine 10 to the host compu-***

***ter 20 via the network interface 18.*")]** It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matters pertains, to include in the system log data to the database, spatial positioning i.e., the geographical locations of the individual gaming machines e.g., casinos offer various promotions and sweepstakes throughout the day. The proximity of gaming machines by front and rear entrances juxtaposed between middle isles, allow casinos and merchants to capitalize on different customers habits or impulsive desires. Moreover, the proximity, to other gaming and gambling events allows them to further capitalize on different customers wants and needs. The inclusion of such data pertaining to the different geographical location of different gaming machines, allows casino owners and merchants to further monitor and predict customer habits and gaming desire, as well as add to their own bottom-line.

## Conclusion

13. The prior art made of record and (listed of form **PTO-892**) not relied upon is considered pertinent to applicant's disclosure as follows. Applicant or applicant's representative is respectfully reminded that in process of patent prosecution i.e., amending of claims in response to a rejection of claims set forth by the Examiner per Title 35 U.S.C. The patentable novelty must be clearly shown in view of the state of the art disclosed by the references cited and any objections made. Moreover, applicant or applicant's representative must clearly show how the amendments avoid or overcome such references and objections. *See* **37 CFR § 1.111(c)**.

# Correspondence Information

14. Any inquiries concerning this communication or earlier communications from the examiner should be directed to **Michael B. Holmes** who may be reached via telephone at **(703) 308-6280**. The examiner can normally be reached Monday through Friday between 8:00 a.m. and 5:00 p.m. eastern standard time.

If you need to send the Examiner, a facsimile transmission regarding After Final issues, please send it to **(703) 746-7238**. If you need to send an Official facsimile transmission, please send it to **(703) 746-7239**. If you would like to send a Non-Official (draft) facsimile transmission the fax is **(703) 746-7240**. If attempts to reach the examiner by telephone are unsuccessful, the **Examiner's Supervisor**, **Anil Khatri**, may be reached at **(703) 305-0282**.

Any response to this office action should be mailed too:

**Director of Patents and Trademarks Washington, D.C. 20231**. Hand-delivered responses should be delivered to the Receptionist, located on the fourth floor of **Crystal Park II, 2121 Crystal Drive Arlington, Virginia.**

***Michael B. Holmes***
Patent Examiner
Artificial Intelligence
Art Unit 2121
United States Department of Commerce
Patent & Trademark Office